REMARKS

Applicant hereby amends claim 1 to correct informalities. Claims 1-41 are pending in this application.

Amended Claim 1

Applicant amends claim 1 to correct informalities. These amendments are not made for reasons related to patentability. Moreover, these amendments per se do not necessitate the introduction of a new ground of rejection; for example, neither the Examiner's arguments nor Applicant's reasoning relies upon the language deleted by these amendments.

Objected-to Claims 6-13, 17, 19, 26-28, and 35-37

The Examiner objected to claims 6-13, 17, 19, 26-28, and 35-37 as dependent upon a rejected base claim, but allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

§ 103(a) Rejection of Claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 over *Akiyama et al.* and *Halter et al.*

Applicant respectfully traverses the rejection of claims 1-5, 14-16, 18, 20-25, 29-34, and 38-41 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,784,464 to Akiyama et al. ("*Akiyama et al.*") in view of U.S. Patent No. 5,319,705 to Halter et al. ("*Halter et al.*").

Claims 1-41 are allowable over *Akiyama et al.* and *Halter et al.* because these references do not teach or suggest, either alone or in combination, each and every element of independent claim 1, from which claims 2-19 depend, or each and every

element of independent claim 20, from which claims 21-41 depend. For example, *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, "sending the encrypted content key and the second storage key to a key management unit," as recited in claims 1 and 20.

In the Office Action, the Examiner did not clearly explain the pertinence of *Akiyama et al.* and *Halter et al.* to the claim limitations. "When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained ..." 37 C.F.R. § 1.104(c)(2). For example, the Examiner failed to point out where either *Akiyama et al.* or *Halter et al.* allegedly teaches any of the "content key," "first storage key," "content data," and "second storage key" recited in claims 1 and 20 (emphasis added). Moreover, the Examiner makes a conclusory statement that it would have been obvious to combine the invention of *Akiyama et al.* with the key distribution system of *Halter et al.* without any clear explanation of how the Examiner proposes to combine these references (Office Action, paragraph bridging pages 3 and 4). Without knowing what correspondence the Examiner intended between the limitations of the claims and the references relied upon, it is difficult for Applicant to address the Examiner's rejection. Thus, it is respectfully requested that the Examiner designate the particular parts of *Akiyama et al.* and *Halter et al.* relied upon and their individual correspondence to the limitations that are recited in the claims.

Akiyama et al. teaches "a client authenticating system in a data distributing system having a data supplying apparatus for holding data and a client receiving the

data distributed via a communication interface from the data supplying apparatus. The data supplying apparatus comprises a key outputting unit for outputting a first key corresponding to the client, a random-number generating element for generating a random number in response to an access request from the client, and a first encrypting element for encrypting the random number with said first key and thereby outputting a first authenticator. The data supplying apparatus further comprises a first transmitting element for transmitting the random number to the client, a first receiving element for receiving a second authenticator from the client and a comparing element for comparing the first and second authenticators with each other and, if the two authenticators are coincident with each other, authenticating the access request from the client." (Col. 2, lines 46-62.)

The client of *Akiyama et al.* comprises "an access requesting element for making an access request to the data supplying apparatus and a second receiving element for receiving the random number transmitted from the data supplying apparatus. The client further comprises a key holding element for holding a second key identical with the first key, a second encrypting element for encrypting the random number with the second key and thereby outputting the second authenticator and a second transmitting element for transmitting the second authenticator to the data supplying apparatus." (Col. 2, line 62 to col. 3, line 5). "The data supplying apparatus may be constructed to distribute, only when the comparing element determines that the two authenticators are coincident with each other, the data to the client." (Col. 3, lines 12-15.)

"The data supplying apparatus may be also constructed to distribute the encrypted data to the client. In this case, the client is constructed to include a first

decrypting element for decrypting the encrypted data. The data supplying apparatus may be constructed to include a third encrypting element for encrypting the third key for decrypting the data by use of the first key. In this case, the client is constructed to include a second decrypting element for decrypting the encrypted third key by use of the second key. Then, the first decrypting element decrypts the encrypted data with the third key decrypted by the second decrypting element." (Col. 3, lines 16-28.)

However, transmitting the second authenticator to the data supplying apparatus, as performed by the client of *Akiyama et al.*, does not constitute "sending the encrypted content key and the second storage key to a key management unit," as required by claims 1 and 20 (emphasis added). Transmitting a single "authenticator" does not constitute sending both the "encrypted content key" and the "second storage key" that are recited in claims 1 and 20.

Although the Examiner additionally relies upon col. 4, lines 12-38, of *Akiyama et al.* for an alleged suggestion that "multiple keys can be generated" (Office Action, pg. 3, paragraph 3), there is no such teaching or suggestion at that section of *Akiyama et al.* Indeed, the section of *Akiyama et al.* relied upon by the Examiner repeats that the client "transmits the second authenticator to the data supplying apparatus" (col. 4, lines 27-29; emphasis added).

Halter et al. does not make up for the deficiencies of *Akiyama et al.* because *Halter et al.* also fails to teach or suggest "sending the encrypted content key and the second storage key to a key management unit," as recited in claims 1 and 20.

Halter et al. teaches "a cryptographic means for protecting software distributed over an open channel or via a high-density stamped medium" (col. 5, lines 28-30).

"When a customer purchases multimedia software from a software distribution facility, the customer provides his/her customer number. The customer key is produced from a set of variables consisting of an assigned customer number, a counter (arbitrarily set to zero), and a secret key-generating key (KGK) known only to the software distribution center. A special copy-right protected function (f) is then used to derive a variant customer key (KC') from the customer key. The data key(s) associated with the multimedia file(s) purchased by the customer are then encrypted with the variant customer key. The clear customer key and the encrypted file key(s) are provided to the customer . . . At the user processor, the keys and encrypted file(s) are initialized and made available to the file recovery program. The file recovery program decrypts and recovers the file(s)." (Col. 5, line 65 to col. 6, line 16.)

However, there is not any teaching or suggestion in *Halter et al.* of "sending the encrypted content key and the second storage key to a key management unit," as required by claims 1 and 20 (emphasis added). For example, the single customer number that the customer of *Halter et al.* provides to the software distribution facility does not constitute "the encrypted content key and the second storage key." Thus, *Halter et al.* fails to teach or suggest "sending the encrypted content key and the second storage key to a key management unit," as recited in claims 1 and 20.

Moreover, it would not have been obvious to one of ordinary skill to combine *Akiyama et al.* and *Halter et al.* to derive the method of claim 1 or the system of claim 20, as suggested by the Examiner, because there is not any motivation to do so. Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or

motivation to do so. *In re Kahn*, 441 F.3d 977, 986, 78 USPQ2d 1329, 1335 (Fed. Cir. 2006).

The Examiner argues, "it would have been obvious . . . to modify the invention of Akiyama et al. by using the key distribution system disclosed by Halter, in order to prevent files from being decrypted except at appropriate user processors" (Office Action, paragraph bridging pages 3 and 4). However, *Halter et al.* does not use any "key distribution" system to prevent files from being decrypted except at appropriate user processors. Instead, *Halter et al.* teaches that a "Generate Variant Customer Key (GVCK) function 116 . . . provide[s] a means whereby encrypted multimedia files cannot be decrypted except at a user processor with a capability for multimedia file recovery" (col. 15, lines 30-32 and lines 47-51, Fig. 4, and Fig. 11; emphasis added). This GVCK function does not constitute any part of the "key distribution" system of *Halter et al.* Thus, there is not any motivation to combine *Akiyama et al.* and *Halter et al.* as suggested by the Examiner.

As explained above, *Akiyama et al.* and *Halter et al.* fail to teach or suggest, alone or in combination, each and every element of independent claims 1 and 20. There is also no motivation to combine these references as suggested by the Examiner to derive the subject matter recited in claims 1 and 20. Thus, claims 1 and 20, and claims 2-19 and 21-41, which depend therefrom respectively, should be allowed over *Akiyama et al.* and *Halter et al.* under 35 U.S.C. § 103(a).

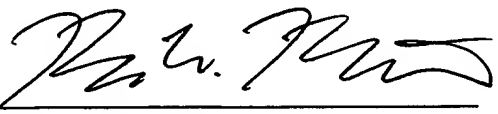
In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 14, 2007

By: 

Reece Nienstadt
Reg. No. 52,072